+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 17/09/2026

S'inscrire

Formation Certification GIAC GICSP

5 jours (35 heures)

Présentation

La formation Certification GIAC GICSP prépare à la certification officielle Global Industrial Cyber Security Professional GICSP et vous permet de maîtriser la cybersécurité des environnements OT et ICS, des architectures industrielles et des réponses aux incidents.

Les systèmes industriels associent automates PLC, interfaces HMI, SCADA, réseaux de terrain et postes d'ingénierie. Leur protection requiert une approche adaptée aux impératifs de disponibilité, de sûreté et de continuité des opérations.

Cette formation vous prépare à l'examen officiel Global Industrial Cyber Security Professional GICSP en couvrant les compétences attendues pour comprendre les architectures ICS, analyser les surfaces d'attaque, sécuriser les communications industrielles et construire des défenses pertinentes.

Vous apprendrez à cartographier un environnement OT, à distinguer les rôles des équipements industriels, à appliquer une segmentation réseau fondée sur les zones et conduits, et à sécuriser les échanges utilisant des protocoles tels que Modbus, DNP3 et OPC UA.

À travers des mises en situation, vous développerez les réflexes nécessaires pour détecter une activité anormale, investiguer un incident sans compromettre le procédé, organiser la remédiation et mobiliser les principes de la norme IEC 62443 dans une démarche de défense en profondeur.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre les architectures, actifs et contraintes des environnements OT et ICS
- Analyser les risques, surfaces d'attaque et menaces propres aux systèmes industriels
- Concevoir une segmentation réseau fondée sur les zones, conduits et principes de défense en profondeur
- Surveiller les protocoles industriels et qualifier des signaux de compromission
- Préparer une réponse à incident adaptée aux enjeux de disponibilité et de sûreté
- Se préparer aux domaines de compétences évalués par la certification Global Industrial Cyber Security Professional GICSP

Public visé

- Administrateur systèmes et réseaux
- Ingénieur cybersécurité OT
- Ingénieur automatisme
- Analyste SOC
- Responsable sécurité des systèmes industriels

Pré-requis

- Connaissances des fondamentaux des réseaux TCP/IP
- Expérience des environnements Windows ou Linux
- Notions d'administration réseau, de pare-feu et de journalisation
- Connaissances générales de la cybersécurité et de la gestion des incidents
- Familiarité avec les systèmes industriels SCADA, PLC ou HMI recommandée

Pré-requis techniques

- PC équipé de Windows 10 ou Windows 11, ou d'une distribution Linux récente
- Processeur 64 bits, 16 Go de RAM recommandés et 40 Go d'espace disque disponible
- Possibilité d'exécuter une machine virtuelle avec VirtualBox 7 ou VMware Workstation
- Connexion Internet stable sans filtrage bloquant les téléchargements, la visioconférence ou les machines virtuelles
- Navigateur Google Chrome ou Mozilla Firefox à jour

Programme de notre formation GIAC GICSP

[Jour 1 - Matin]

Fondamentaux des systèmes industriels et de l'OT

- Positionnement de la certification Global Industrial Cyber Security Professional GICSP® et logique de préparation à l'examen
- Différences entre environnements IT, OT, ICS et systèmes cyberphysiques

- Contraintes industrielles de disponibilité, sûreté, intégrité du procédé et maintien en conditions opérationnelles
- Rôles des PLC, RTU, HMI, serveurs SCADA, historiens et postes d'ingénierie
- Cycle de vie d'un système de contrôle industriel, de la conception à l'exploitation

[Jour 1 - Après-midi]

Architectures ICS et inventaire des actifs

- Lecture d'une architecture industrielle selon les niveaux du modèle Purdue
- Identification des flux entre terrain, contrôle, supervision, DMZ industrielle et système d'information
- Cartographie des actifs critiques, dépendances, accès distants et points de concentration
- Analyse des écarts entre exigences de cybersécurité, production et sûreté de fonctionnement
- Atelier pratique : cartographier une architecture SCADA fictive, identifier les actifs critiques et qualifier les flux IT et OT.

[Jour 2 - Matin]

Protocoles OT et surfaces d'attaque industrielles

- Fonctionnement des communications Modbus, DNP3, OPC UA et protocoles Ethernet industriels
- Analyse des notions de téléconduite, commandes, télémesures, alarmes et échanges de configuration
- Faiblesses courantes liées à l'absence d'authentification, de chiffrement ou de contrôle d'intégrité
- Exposition des postes d'ingénierie, services distants, interfaces web, supports amovibles et équipements sans fil
- Vecteurs d'attaque affectant les automates, interfaces opérateurs et serveurs de supervision

[Jour 2 - Après-midi]

Segmentation et défense en profondeur

- Principes de séparation entre réseau bureautique, DMZ industrielle et zones de contrôle
- Construction de zones de sécurité et de conduits selon IEC 62443
- Usage des pare-feu, VLAN, ACL, passerelles sécurisées et flux explicitement autorisés
- Sécurisation des accès fournisseurs, de la maintenance distante et des échanges avec l'historien
- Atelier pratique : concevoir une matrice de flux et une segmentation par zones et conduits pour une ligne de production.

[Jour 3 - Matin]

Menaces et vulnérabilités dans les environnements OT

- Panorama des menaces visant les infrastructures critiques, chaînes de production et installations distribuées
- Scénarios de compromission par hameçonnage, rebond depuis l'IT, accès distant, équipement exposé ou prestataire
- Impacts possibles sur le procédé, la disponibilité, la qualité, l'environnement et la sécurité des personnes
- Gestion des vulnérabilités, des correctifs et des changements dans un contexte industriel contraint
- Mesures de réduction de l'exposition, comptes par défaut, services inutiles et accès non maîtrisés

[Jour 3 - Après-midi]

Durcissement des composants et contrôle des accès

- Durcissement des postes opérateurs, serveurs SCADA et stations d'ingénierie
- Gestion des identités, privilèges, comptes de service et accès à forte responsabilité
- Application de listes d'autorisation, contrôle applicatif et protection contre les supports amovibles
- Stratégies de sauvegarde, restauration, configuration de référence et validation des changements
- Atelier pratique : analyser une station d'ingénierie compromise et proposer un plan de durcissement priorisé.

[Jour 4 - Matin]

Détection et supervision de la sécurité OT

- Définition d'une ligne de base des communications et comportements normaux du procédé
- Collecte des journaux depuis les serveurs, postes, équipements réseau et outils de sécurité
- Détection des anomalies de protocole, commandes inhabituelles, changements de logique et mouvements latéraux
- Positionnement des sondes réseau, IDS industriels et points de surveillance aux frontières de zones
- Corrélation des événements OT et IT dans une démarche de supervision et d'investigation

[Jour 4 - Après-midi]

Réponse à incident en environnement industriel

- Adaptation du cycle de réponse à incident aux exigences de disponibilité et de sûreté industrielle
- Qualification d'une alerte, préservation des preuves et coordination entre SOC, exploitation et ingénierie
- Décisions de confinement, continuité du procédé, retour à un état maîtrisé et communication de crise
- Plans de réponse pour ransomware, accès distant non autorisé, modification de configuration et perte de visibilité
- Atelier pratique : piloter la réponse à un incident simulé affectant une HMI et un réseau de supervision.

[Jour 5 - Matin]

Gouvernance, risques et IEC 62443

- Gouvernance de la cybersécurité industrielle et responsabilités des équipes IT, OT, sécurité et fournisseurs
- Évaluation des risques selon la criticité des actifs, les conséquences physiques et les scénarios de menace
- Principes de IEC 62443, niveaux de sécurité, exigences système et gestion du cycle de vie
- Formalisation d'un inventaire, d'exigences de sécurité et d'une feuille de route de remédiation
- Révision structurée des domaines de connaissances attendus pour l'examen GICSP

[Jour 5 - Après-midi]

Consolidation et préparation à l'examen

- Révision des concepts clés relatifs aux composants ICS, protocoles, architectures et défenses réseau
- Analyse de questions de préparation sans reproduction de contenu d'examen confidentiel
- Méthode de lecture des scénarios, hiérarchisation des risques et élimination des réponses incohérentes
- Organisation des dernières révisions, gestion du temps et préparation du passage de la certification
- Atelier pratique : résoudre une étude de cas complète combinant architecture OT, menace, détection et plan de réponse.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.